4.8 Specialty Engineering

Specialty Engineering is a subset of System Engineering (SE) that defines and evaluates specific areas, features, and/or characteristics of a system. Specialty Engineering supplements the acquisition process by defining these characteristics and assessing their impact on the program. SE relies on specialty domain expertise to define and characterize specific requirements. SE's function in this process is to integrate the design engineer and specialty engineer's activities, coordinate and open communication lines between the design engineer and specialty engineer, and focus the engineering effort toward the common goal of satisfying the customer—not to perform detailed Specialty Engineering work.

Analysis of the system is a primary means of conducting Specialty Engineering. These analyses are categorized under Specialty Engineering because they require specialized engineering skills. These specialized skill areas include system safety engineering (SSE); Reliability, Maintainability, and Availability (RMA); Human Engineering (human factors); Electromagnetic Environmental Effects (E^3); quality Engineering; Information Security Engineering; and Hazardous Materials Management/Environmental Engineering. Engineers in these disciplines perform analyses throughout the system's lifecycle. The results are used to derive, validate, and verify requirements; evaluate system design progress and technical soundness; and manage risk. At a minimum, analysis results are available at standard design milestones, including the design, acquisition, and program reviews. The results are communicated via reports. In the case of supplier involvement, deliverables are in accordance with contract requirements. The general process for performing Specialty Engineering is depicted in Figure 4.8-1, which lists the key inputs necessary to initiate the task, providers, process tasks, outputs required, and customers of process outputs.

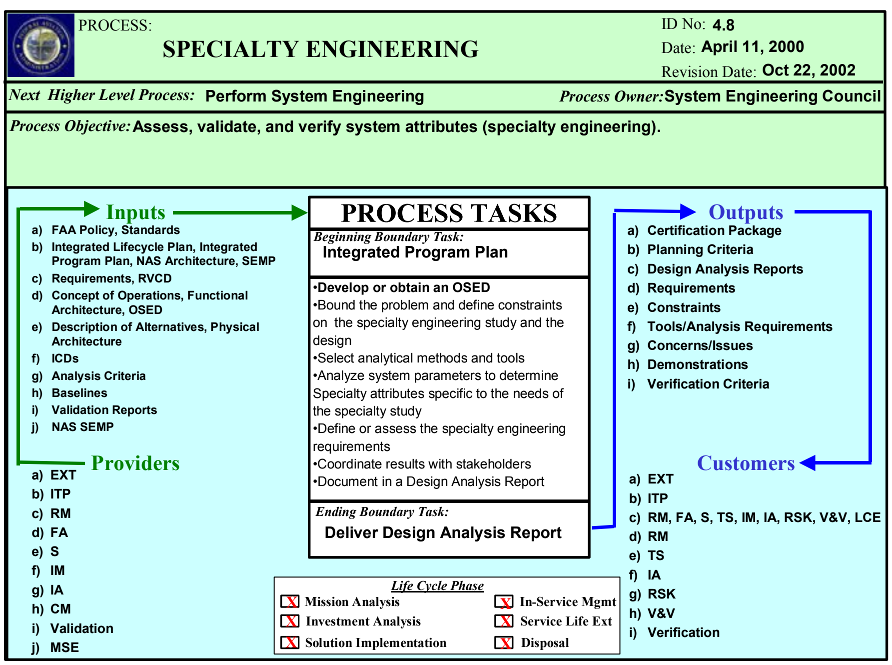

Figure 4.8-1. Specialty Engineering Process-Based Management Chart

4.8.0 Introductory Material

4.8.0.1 Introduction to Specialty Engineering

Specialty Engineering is conducted throughout the system's lifecycle. Specialty Engineering analyses are conducted early to derive and validate requirements. In addition, the Specialty Engineering disciplines support the Trade Studies (Section 4.6), Synthesis (Section 4.5), and Functional Analysis (Section 4.4) efforts in selecting and designing solutions to requirements. Later in the lifecycle, after requirements at all levels are validated, these analyses provide support in verifying the requirements by describing and assessing the characteristics of the design and/or operations. As early as possible in the lifecycle, the Specialty Engineering disciplines find and resolve potential program risk. Finding and controlling risk early assists in seeking the lowest possible cost and increases the probability of program success and operator acceptance of the product.

This section contains a description of the functions, objectives, and products of the various disciplines included in Specialty Engineering.

4.8.0.1.1 Description of Specialty Engineering Disciplines

Specialty Engineering analyses provide characteristics of the system from a specific technical perspective. Table 4.8-1 provides a general description of the Specialty Engineering disciplines.

Table 4.8-1. Specialty Engineering Disciplines

Specialty Engineering Discipline	Description
SSE	Evaluation and management of the safety risk associated with a system using measures of safety risk identified in various hazard analyses, fault tree analyses, safety risk assessments, and hazard tracking and control.
RMA	Quantitative and qualitative analyses of the attributes of the system to perform reliably. Quantitative assessments are in the form of probabilistic, mean, and/or distribution assessments. Qualitative analyses are in the form of failure mode assessments. Evaluation of the design's ability to meet operational readiness requirements through preventive and corrective maintenance.
Human Factors Engineering	Human factors is a multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to: – equipment, systems, facilities – procedures, jobs, environments – staffing – training

Specialty Engineering Discipline	Description
	– personnel and organizational management for safe, comfortable, and effective human performance.
E^3	Analysis of the system for susceptibility and/or vulnerability to electromagnetic fields or capability to generate such fields that might interfere with other systems, identify sources of interference, and means for correction within the levels prescribed by law, program requirements, spectrum management, or recognized standards. E^3 is composed of Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC)
Quality Engineering	Evaluation of a system's ability to meet its requirements and to mitigate product defects.
Information Security Engineering	Evaluation of the vulnerability of the system to unauthorized access and use, or susceptibility to sabotage. Assessment of the ability of the system to survive a security threat in the expected operational environment.
Hazardous Materials Management/Environmental Engineering	Determination of environmental impacts at deployment sites and during operations, including both environmental impacts on the system and system impacts on the environment during all phases of the product life.

In addition to resolving problems and defining requirements early, Specialty Engineering supplies information to the other SE functions, including Requirements Management (Section 4.3), Risk Management (Section 4.10), Configuration Management (Section 4.11), and Validation and Verification (Section 4.12). The major relationships between Specialty Engineering and other SE processes are depicted in Figure 4.8-2.

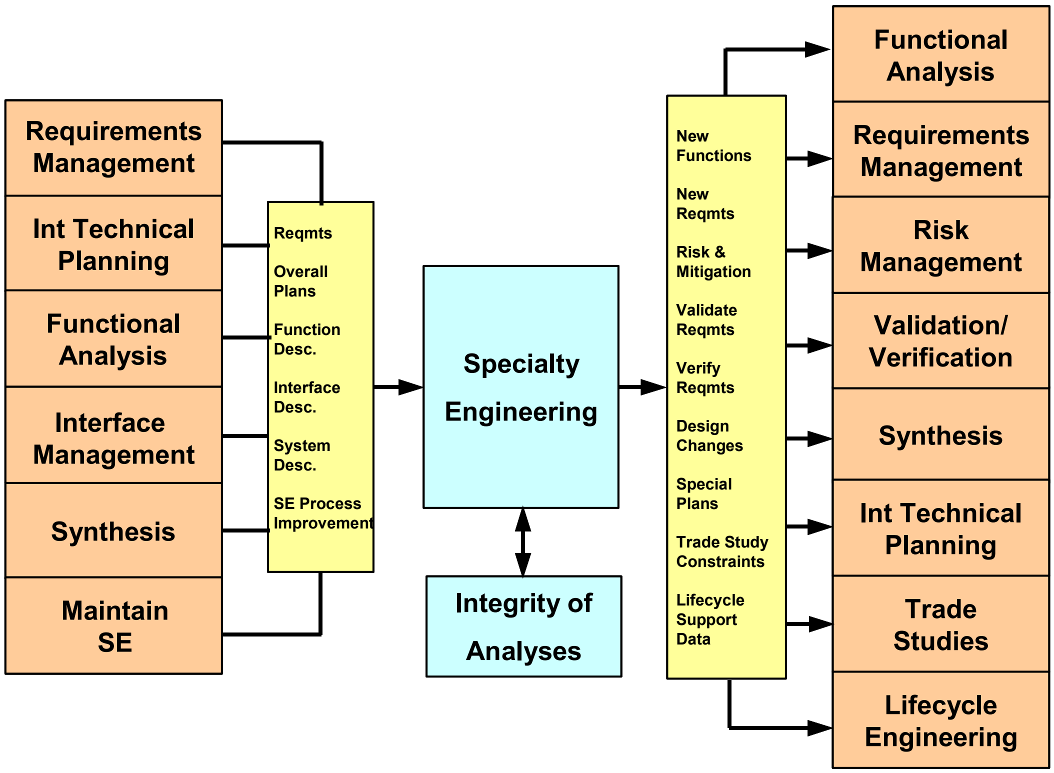

Figure 4.8-2. Major relationships Between System Engineering Elements and Specialty Engineering

The relationships depicted in Figure 4.8-2 are further described in Table 4.8-2.

Table 4.8-2. Major Effects of Specialty Engineering on Other System Engineering Processes

Affected SE Process	How Affected
Integrated Technical Planning (Section 4.2)	The Integrated Technical Planning process feeds Specialty Engineering. Integrated Technical Planning produces the plans for Specialty Engineering, SE, and all other SE processes. The plans detail what is to be done, who is to do it, the standards of performance, and when each task is to be performed.
Requirements Management (Section 4.3)	The Requirements Management process both feeds and is fed by Specialty Engineering. The system under study is described in order to perform Specialty Engineering analyses. Requirements are a key component of any description and they are an output of the Requirements Management process. Specialty Engineering studies often find characteristics that create a need for new or different requirements. Sometimes, the Specialty Engineering disciplines find areas of conflict between two or more requirements. In either case, the Specialty Engineering function develops the new or changed requirements and these are an input to the Requirements Management process.
Functional Analysis (Section 4.4)	The Functional Analysis process both feeds and is fed by Specialty Engineering. To execute a Specialty Engineering

Affected SE Process	How Affected
	analysis, the specialist shall have a thorough understanding of the system functions. This understanding is a result of performing a Functional Analysis of the system.
Interface Management (Section 4.7)	Specialty Engineering both feeds and is fed by Interface Management. The system under study is described in order to perform Specialty Engineering analyses. Interface Requirements Descriptions (IRD) are key components of any system description and are an output of the Interface Management process. Specialty Engineering studies often find characteristics that create a need for new or different interface requirements or descriptions. Sometimes, the Specialty Engineering disciplines find areas of conflict between two or more interfaces. In either case, the Specialty Engineering function develops the new or changed requirements, which are inputs to the Interface Management process.
Risk Management (Section 4.10)	Specialty Engineering feeds the Risk Management process. Specialty Engineering studies and analyses are designed to find and assess potential problem areas of a design as early as possible. When a potential problem is found, the information becomes an input to the Risk Management process for mitigation and control.
Configuration Management (Section 4.11)	Specialty Engineering outputs are inputs to the Configuration Management process. During the execution of Specialty Engineering analyses, it may be discovered that additional or changed design features are required, or changes to operating, maintenance, or installation procedures are needed. When these discoveries occur, the proposed changes become inputs to the Configuration Management process.
Validation and Verification (Section 4.12)	Specialty Engineering outputs feed the Validation and Verification process. Early in the program's lifecycle, Specialty Engineering is used to validate requirements, which is accomplished by comparing the requirements defined in early Specialty Engineering analyses to those defined in current/later analyses. If the Specialty Engineering analyses find a need for an existing requirement, then the requirement may be considered validated. Specialty Engineering feeds Verification Criteria to the Verification process. Specialty Engineering is also used to verify requirements later in the system's lifecycle. Verification may be accomplished either by test or SE Assessment. Specialty Engineering is a form of assessment and may be used to demonstrate verification.

4.8.0.2 Inputs and Providers to Specialty Engineering

Table 4.8-3 depicts the inputs needed to conduct Specialty Engineering analyses.

58 **Table 4.8-3. Specialty Engineering Process Inputs**

Process Input	Input Purpose/Description	From Process
FAA Policy and Standards	Policy and standards, such as the Acquisition Management System (AMS), define what is expected and how well it needs to be done.	AMS and FAA Orders
Integrated Lifecycle Plan	The Integrated Lifecycle Plan provides planning information necessary to support the system throughout its lifecycle.	Integrated Technical Planning (Section 4.2)
Integrated Program Plan (IPP)	The IPP provides information on the overall plan for conducting the program. It provides information on program constraints, system constraints, and Specialty Engineering plans. Each specific program maintains the IPP. It is an aggregate plan that includes and integrates all the program specific plans. The IPP details what tasks are to be performed, who is to do them, and when the tasks are to be performed.	Program's IPP Integrated Technical Planning (Section 4.2)
National Airspace System (NAS) Architecture	The NAS Architecture is the technical blueprint for NAS Modernization and guides the Federal Aviation Administration (FAA) on what systems are planned for modernizing the NAS.	Synthesis (Section 4.5)
System Engineering Management Plan (SEMP)	The SEMP defines the plan for conducting SE in the AMS and the program.	System Engineering in the Acquisition Management System Program Lifecycle (Chapter 3)
Requirements	Requirements provide information about the system's required characteristics, specifications, performance, and requirements. They assist in developing the system description. System requirements are documented in the initial Requirements Documents (iRD), final Requirements Documents (fRD), and system specification(s). The execution teams and SE develop and maintain the requirements documents.	Requirements Management (Section 4.3)
Requirements Verification Compliance Documents (RVCD)	The RVCD records the verification status of all requirements.	Requirements Management (Section 4.3)

Process Input	Input Purpose/Description	From Process
Concept of Operations (CONOPS)	The CONOPS is a user-oriented document that describes system functional characteristics for a proposed system from the user's viewpoint. It explains the existing system, current environment, users, interactions among users and the system, and organizational impacts. The CONOPS document is written in order to communicate overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements.	Functional Analysis (Section 4.4)
Functional Architecture	The Functional Architecture identifies, analyzes, and describes the functions of a system. It provides information required for a system description and assists in the definition of requirements. Functional Analysis is the process of turning a need or system requirement into a description and an architecture of functions (system behaviors or behavior descriptors). The execution teams and/or SE perform and maintain the Functional Architecture.	Functional Analysis (Section 4.4)
Operational Services and Environmental Description (OSED)	The OSED is a comprehensive, holistic Communications, Navigation, and Surveillance (CNS)/Air Traffic Management (ATM) system description. It describes the services, environment, functions, and mechanizations that form a system's characteristics.	Functional Analysis (Section 4.4)
Description of Alternatives	Description of Alternatives is described as Physical Architectures. When performing Trade Studies (Section 4.6), a number of alternatives shall be competitively evaluated.	Synthesis (Section 4.5)
Physical Architecture	Physical Architecture identifies and defines the system and its components, including the physical interfaces among products, subsystems, humans, lifecycle processes, and external interfaces to higher-level systems or interacting systems.	Synthesis (Section 4.5)
Interface Control Document (ICD)	The ICD controls interface design.	Interface Management (Section 4.7)
Analysis Criteria	Criteria for specialty engineering analyses are specified to establish the degree of validation required for the analyses and associated tools, the methods to use to ensure that the data is of the proper quality and range, and the level of documentation required.	Integrity of Analysis (Section 4.9)

Process Input	Input Purpose/Description	From Process
Baselines	When the requirements and design have reached sufficient maturity, they are baselined to facilitate management of the configuration.	Configuration Management (Section 4.11)
Validation Reports	Validation Reports document the results of the Validation effort. They report requirements that are validated and those that are considered nonconforming.	Validation (Section 4.12)
NAS SEMP	The NAS SEMP describes the overall SE used in the FAA.	Manage System Engineering (Section 4.14)

4.8.0.3 General Specialty Engineering Process Tasks

Most, if not all, Specialty Engineering disciplines follow a similar process when conducting associated analyses. The following paragraphs provide general guidance on performing Specialty Engineering in the FAA. These processes are depicted in Figure 4.8-1. The process tasks are:

- Describe the system in physical and/or functional terms. This task has to be completed before the specialists may begin; if not, the specialists may perform this task, as long as it is performed according to the guidance in Functional Analysis (Section 4.4) and Interface Management (Section 4.7)).
- Bound the problem and define Constraints on the Specialty Engineering study and the design.
- Select analytical methods and tools.
- Analyze system parameters to determine specialty attributes specific to the views of the Specialty Engineering study.
- Define or assess the Specialty Engineering Requirements.
- Coordinate results with stakeholders.
- Document the analysis in a Design Analysis Report (DAR).

The following paragraphs detail the process tasks depicted in Figure 4.8-1.

4.8.0.3.1 Task 1: Obtain or Develop an Operational Services and Environmental Description

The first task in performing a Specialty Engineering analysis is to understand and describe the system under study at an appropriate level. The OSED is an excellent source of this information; it is a system description that is developed in the Functional Analysis process (Section 4.4).

It is recommended that the specialty engineer use the existing descriptions to frame the Specialty Engineering analysis. However, there are times when the existing system descriptions are insufficient in detail for the specialist. In these cases, the specialty engineer develops the system description. When developing the system description, the specialty engineer shall comply with the guidance in Functional Analysis and Interface Management (Section 4.7).

Functional Analysis describes the desired behaviors of a system. These behaviors provide critical insight into how the system is intended to perform and, therefore, are a critical input to any Specialty Engineering analysis. To perform an assessment of a system, the engineer is required to understand the functions of that system and be able to relate the specialties to these functions. Normally, the Functional Analysis is completed before the Specialty Engineering process begins, and all that is required of the specialty engineer is to obtain and review the Functional Analysis and use it to enhance or complete the system description. In some cases, either because the engineers failed to perform it or because it is too early in the design process, the Functional Analysis is not available. In these cases, the specialty engineer shall refer to guidance in Functional Analysis and perform the Functional Analysis independently.

4.8.0.3.2 Task 2: Bound the Problem and Define Constraints on the Study and Design

Every system problem or analysis has breadth and depth. The breadth of a system analysis refers to the system boundaries. Boundaries limit the system to elements of the system model that affect or interact with each other in order to accomplish the central mission(s) or function. Depth refers to the level of detail in the description. The level of detail in an analysis varies inversely with the breadth of the system. For a system as broad as the NAS, the description and analysis are general in nature with little detail on individual components. On the other hand, a simple system, such as a valve in a landing gear design, includes significant detail to support the assessment.

Constraints on the design play an important role in the conduct of the analysis and the credibility of the results. It is essential to identify the Constraints before the analysis to account for their influence on the methods used and the alternatives chosen. As part of determining the Constraints, the scope of the analysis, the ground rules, and assumptions are identified. Identifying the customer(s) for the analysis is important with respect to defining the scope. The analysis may be subject to contractual restraints if it is a deliverable; therefore, it is necessary to consider these restraints when defining the scope of the effort. The project schedule and budget may also impose limits on the analysis, which may affect the assumptions and ground rules. The analysis team and the recipients of the report shall be aware of all the scope limitations, ground rules, assumptions, and guidelines that apply to the assessment and product design. The following sources are used to identify Constraints:

- CONOPS defined via Functional Analysis (Section 4.4)
- Contract Statement of Work (SOW), including referenced standards and procedures
- Compliance documents that apply to the analysis methods and report
- Customer-specified requirements on cost, schedule, and product performance
- Management-imposed business goals and Constraints
- Functional, performance, and interface requirements derived from the design concept

- Functional, performance, and interface requirements imposed by the use of commercially available or preexisting hardware and software
- Operational constraints imposed by the user
- Environmental constraints imposed by the physical and operational environment
- Constraints imposed by the production or Verification process (Section 4.12)
- Design constraints imposed by standard practices that are defined by the government or standards-setting bodies

4.8.0.3.3 Task 3: Select Analytic Methods and Tools

To ensure Integrity of Analyses (Section 4.9), the engineer selects analytic methods and tools that meet the program phase; the system analysis needs; and cost, schedule, and skill constraints. It is important to select methods and tools that match the analysis objectives within the resource limitations of the effort.

4.8.0.3.4 Task 4: Analyze System Parameters To Determine System Attributes

In this step, the attributes of the design are determined by using the methods and tools appropriate to the Specialty Engineering discipline. The appropriate guidelines and handbooks for each Specialty Engineering discipline are listed in Table 4.8-4. The AMS FAA Acquisition System Toolset (FAST) often contains guidelines for these activities. For example, it is recommended that the team, if conducting a safety assessment, consult the FAA System Safety Handbook (SSH) and the NAS System Safety Management Plan (SSMP) found in the FAST. For some analyses, it is recommended that the results include programmatic attributes, such as cost and schedule impacts, as appropriate to the analysis.

In addition, the SE or project team, as part of this process, conducts technical or peer reviews of the analysis and its results. The technical community conducts this independent evaluation before the Specialty Engineering DARs are submitted.

The results of Specialty Engineering analyses confirm design attributes necessary for acceptable product performance, cost, schedule, and risk. When an attribute is not confirmed, the analysis and/or the baseline shall be revised.

Revision may be implemented through changes in scope, ground rules, assumptions, and analytic methods. The analysis process is reactivated with the intent of determining an alternative result that is acceptable and valid. Alternatively, the results of the analysis may drive revision of the Requirements or design Baseline. This revision is accomplished by preparing appropriate change proposal documentation for input to the Configuration Management process (Section 4.11).

163 **Table 4.8-4. Guidelines and Handbooks for Conducting Specialty Engineering**

Phase	Analysis	Guidance/Reference
Mission Analysis	E^3 EMC requirements	FAST. (2000). Environment/Energy/ Safety/Health. http://fast.faa.gov/ FAST. (2000). Radio Spectrum Management. http://fast.faa.gov/
	Environmental Requirements Analysis	FAST.[1] Environment/Energy/Safety /Health. http://fast.faa.gov/
	Human Factors Functional Analysis	FAST. Human Factors. http://fast.faa.gov/
	Human Factors System (Mission) Analysis	FAST. Human Factors. http://fast.faa.gov/
	Maintainability Requirements Analysis	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Operational Safety Assessment (OSA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH[2], Chapter 4. NAS SSMP[3], Chapters 3 and 4.
	Reliability Requirements Analysis	(Reserved)
Investment Analysis	Comparative Safety Assessment (CSA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 4 NAS SSMP
	EMC Control Plan	FAST. (2000). Environment/Energy/ Safety/Health. http://fast.faa.gov/ FAST. (2000). Radio Spectrum Management. http://fast.faa.gov/
	Human Factors Function Allocation	FAST. Human Factors. http://fast.faa.gov/

[1] Federal Aviation Administration, Federal Acquisition System Tools (FAST), Office of Research and Acquisitions (ARA), [On-line] Available: http://fast.faa.gov.

[2] U.S. Federal Aviation Administration, "FAA System Safety Handbook," FAA Office of System Safety (ASY), Washington, D.C. (2000).

[3] U.S. Federal Aviation Administration, "NAS Modernization System Safety Management Plan," FAA Office of Architecture and SE (ASD), Washington, D.C. (2000).

Phase	Analysis	Guidance/Reference
	Human Factors Program Plan	FAST. Human Factors. http://fast.faa.gov/
	Maintainability Plan	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Preliminary Hazard Analysis (PHA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 NAS SSMP
	Quality Engineering Plan	FAST. Quality Assurance. http://fast.faa.gov/
	Reliability Program Plan	(Reserved)
	Specialty Engineering Support of Trade Studies or Alternatives Analysis	FAST. Investment Analysis. http://fast.faa.gov/ Synthesis of Alternatives (Section 4.8)
	System Safety Program Plan (SSPP)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 5 NAS SSMP
	Environmental/ Hazardous Material Analysis	FAST. Environment/Energy/Safety /Health. http://fast.faa.gov/
Solution Implementation	Failure Modes and Effects Analysis (FMEA)	(Reserved)
	Failure Modes and Effects Criticality Analysis (FMECA)	(Reserved)
	Failure Reporting Analysis and Corrective Action System (FRACAS)	(Reserved)
	Failure Review Board	(Reserved)
	Hazard Tracking and Risk Resolution	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 3 NAS SSMP
	Human Factors Demonstrations, Models, and Mockups	(Reserved)

Phase	Analysis	Guidance/Reference
	Human Factors Error Analysis	(Reserved)
	Human Factors Operational Sequence Diagrams	(Reserved)
	Human Factors Operator Task Analysis	(Reserved)
	Human Factors Timeline Analysis	(Reserved)
	Human Factors Workload Analysis	(Reserved)
	Maintainability Analysis	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Maintainability Demonstration	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Maintainability Modeling	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Maintenance Task Analysis	FAST. Sustainment and Maintenance. http://fast.faa.gov/
	Operating and Support Hazard Analysis (O&SHA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 NAS SSMP
	Reliability Centered Maintenance (RCM)	(Reserved)
Solution Implementation	Reliability Development Growth Testing (RDGT)	(Reserved)
	Reliability Modeling	(Reserved)
	Sneak Circuit Analysis	(Reserved)
	Subsystem Hazard Analysis (SSHA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 NAS SSMP
	System Hazard Analysis (SHA)	FAST. System Safety Management. http://fast.faa.gov/ FAA SSH, Chapter 8 NAS SSMP

164

4.8.0.3.5 Task 5: Define and Document Specialty Engineering Requirements

The Specialty Engineering products described in "Task 4: Analyze System Parameters to Determine System Attributes" (Paragraph 4.8.0.3.4) result in the definition and assessment of Specialty Engineering-related Requirements. These Requirements shall meet the standards for requirements definition and documentation described in Requirements Management (Section 4.3). In addition, these Requirements shall be validated and verified, as described in Validation and Verification (Section 4.12).

4.8.0.3.6 Task 6: Coordinate Results With Stakeholders

The results of the Specialty Engineering process (particularly the DARs and Requirements) shall be coordinated with the project/program stakeholders. This coordination is conducted in both formal and informal forums. The informal forums include peer reviews and working groups. The formal forums include Acquisition Reviews and Design Reviews, as described in Integrated Technical Planning (Section 4.2).

4.8.0.3.7 Task 7: Document the Specialty Engineering Analysis in a Design Analysis Report

The primary output of any Specialty Engineering function is the DAR, which documents the results of the specific analysis with rationale. Each DAR shall contain the following results:

- Description of the system's special characteristics
- List of existing Requirements that were either validated or verified in the analysis
- Residual risks
- Candidate Requirements found as a result of the analysis

These Requirements are inputs to the Requirements Management process (Section 4.3) and shall be considered for inclusion in iRD and fRD. The rationale includes the scope, ground rules, assumptions, constraints, methods, and tools applicable to the analysis.

The Specialty Engineering outputs are often used to validate and/or verify requirements. In addition, change proposal documentation is produced if the conclusions of the analysis call for a revision to the Requirements or design Baseline. This revision is an input to the Configuration Management process (Section 4.11) for authorization to change the Baseline as the analysis indicates.

Requirements for contents and format may be applicable to the DAR as specified by the contract. Figure 4.8-3 provides a sample outline of the contents of the DAR.

1.0 Executive Summary
2.0 Introduction
3.0 Summary of results
4.0 Summary of conclusions (including residual risks)
5.0 Recommendations (including mitigation)
6.0 System Description
    6.1 Summary
    6.2 Operational Services and Environment Description (OSED)
    6.3 Functional Analysis (if applicable)
    6.4 Requirements (if applicable)
7.0 Description of system special characteristics (detailed analysis worksheets or data)
8.0 List of candidate requirements
9.0 List of requirements that were validated and/or verified with rationale
10.0 Analysis methodology with rationale

Figure 4.8-3. Sample Outline of a Design Analysis Report

4.8.0.4 Outputs of Specialty Engineering

The following paragraphs describe the outputs of Specialty Engineering. The outputs are:

- Certification Package
- Planning Criteria
- DARs (specific to the Specialty Engineering study)
- Specialty Engineering Requirements
- Constraints
- Tools/Analysis Requirements
- Concerns/Issues
- Demonstrations
- Verification Criteria

4.8.0.4.1 Certification Package

Reserved

4.8.0.4.2 Planning Criteria

Any Planning Criteria necessary for performing Specialty Engineering throughout the remainder of the program's lifecycle need to be provided to the Integrated Technical Planning process (Section 4.2)

4.8.0.4.3 Design Analysis Report

The DAR is the means of documenting and reporting the methods and results of the Specialty Engineering analyses. Figure 4.8-3 provides a sample outline of a DAR.

4.8.0.4.4 Specialty Engineering Requirements

In the course of performing an analysis, the specialty engineer typically defines, validates, or verifies Requirements. Occasionally, the specialist discovers characteristics of the system that are not adequately specified in the existing Requirements or specification documents. If this occurs, the specialist defines those necessary Requirements consistent with the specialist's area of expertise and the requirements standards described in Requirements Management (Section 4.3).

4.8.0.4.5 Constraints

Constraints necessary for performing Specialty Engineering throughout the remainder of the program's lifecycle need to be provided to the Trade Studies process (Section 4.6).

4.8.0.4.6 Tools/Analysis Requirements

Tools/Analysis Requirements for performing Specialty Engineering throughout the remainder of the program's lifecycle need to be provided to the Integrity of Analyses process (Section 4.9).

4.8.0.4.7 Concerns/Issues

Appendix D contains guidance on Concerns/Issues as a product of Specialty Engineering.

4.8.0.4.8 Demonstrations

Demonstrations are often used to verify compliance with Requirements in servicing, reliability, maintainability, transportability, and human factors engineering. Demonstrations are used to verify what is accomplished by operating, adjusting, or reconfiguring items performing their design functions under specific scenarios. The items may be instrumented and quantitative limits of performance monitored; however, only check sheets are required rather than recordings of actual performance data. This method is used when actual demonstration techniques may be used to verify compliance with a Requirement. Observations made by engineers or instrumentation are compared with predetermined responses based on the requirements. An example of this verification method is the demonstration of installing and uninstalling an aircraft engine in a required amount of time.

Demonstrations may also be used to validate unstable Requirements. If there is a risk inherent to a Requirement, Demonstrations may be used to determine the correct characteristics needed.

"Test and Evaluation Verification" (Paragraph 4.12.2.2.1,Verification by Demonstration) has more information on Demonstrations.

4.8.0.4.9 Verification Criteria

The specialist may be called upon to define specific verification requirements, as described in "Step 3: Develop Verification Approach" (Paragraph 4.12.2.5.2.2.3). The Verification Criteria or requirements are added to the Verification Requirements Traceability Matrix (VRTM).

4.8.0.5 Specialty Engineering Tools

The tools used in Specialty Engineering are often unique to each Specialty Engineering discipline. They include databases, drawing tools, requirements and Functional Analysis tools, word and document processors, and spreadsheets. The selection of specific tools depends on criteria established by the particular program. These tools are identified and controlled as documented in individual Specialty Engineering plan sections of the IPP.

4.8.0.6 Specialty Engineering Process Metrics

The schedule completion of Specialty Engineering analyses measured against the plan is a measure of the degree to which these analyses are being effectively managed. The effectiveness of Specialty Engineering analyses may be measured by the rework of analyses or incompatibility with measured performance as an indication that these analyses are reaching inaccurate conclusions.

Of the seven general measurement categories discussed in section, the five that are applicable to Specialty Engineering are Schedule and Progress, Resources and Cost, Process Performance, Customer Satisfaction, and Product Quality. These measures, along with other candidate measures for Specialty Engineering, are provided in Table 4.8-5. It is recommended that each effort tailor these measures and add other applicable project-specific measures to ensure the contribution of necessary information to the decisionmaking processes.

Table 4.8-5. Candidate Measures for Specialty Engineering*

Schedule and Progress	Resources and Cost	Product Size and Stability	Product Quality	Process Performance	Technology Effectiveness	Customer Satisfaction
Achievement of specific milestone dates	Total effort compared to plan	Documentation of special engineering characteristics	Technical performance	Process productivity	Technology impact on product	Customer survey results
Test status	Resource utilization	Requirements	Defects	Process activity cycle time	Baseline changes	Performance rating
Percent of analysis studies completed (schedule/progress)		Percent of requirements derived from specialty analyses	Standards compliance	Depth of the specialty analyses as a percentage versus the target depth		

*NOTE: The measures above and only general examples to indicate the type of information that might be included in the individual section measurement matrix.

4.8.1 System Safety Engineering

SSE (also called Safety Risk Management) is a Specialty Engineering discipline within SE. It is recommended that system/safety engineers and program managers refer to the FAA SSH and the NAS Modernization SSMP for detailed information regarding the planning and conduct of SSE. The following paragraphs describe how system safety is integrated into a system's overall SE.

4.8.1.1 What Is System Safety Engineering?

SSE is the application of engineering and management principles, criteria, and techniques to optimize the safety of a system within the program's operational and programmatic constraints. These engineering and related management tools are used to identify, evaluate, and control hazards associated with a system. A hazard is a real or likely event that has the potential to harm people or damage the system. SSE's goal is to identify the hazards in a system early and continuously, to assess the risk (severity and likelihood) of each hazard, and to actively control the highest risk hazards. The NAS Modernization SSMP, Figure 4.2-1 (Risk Assessment Matrix) under the Safety Risk Management hyperlink in the FAST (http://fast.faa.gov/toolsets/index.htm), provides more information on this topic, as do Table 4.2.1 (Severity Definitions) and Table 4.2-2 (Likelihood or Probability Definitions).

As illustrated in Figure 4.8-4, the SSE process is a closed loop method of Risk Management (Section 4.10).

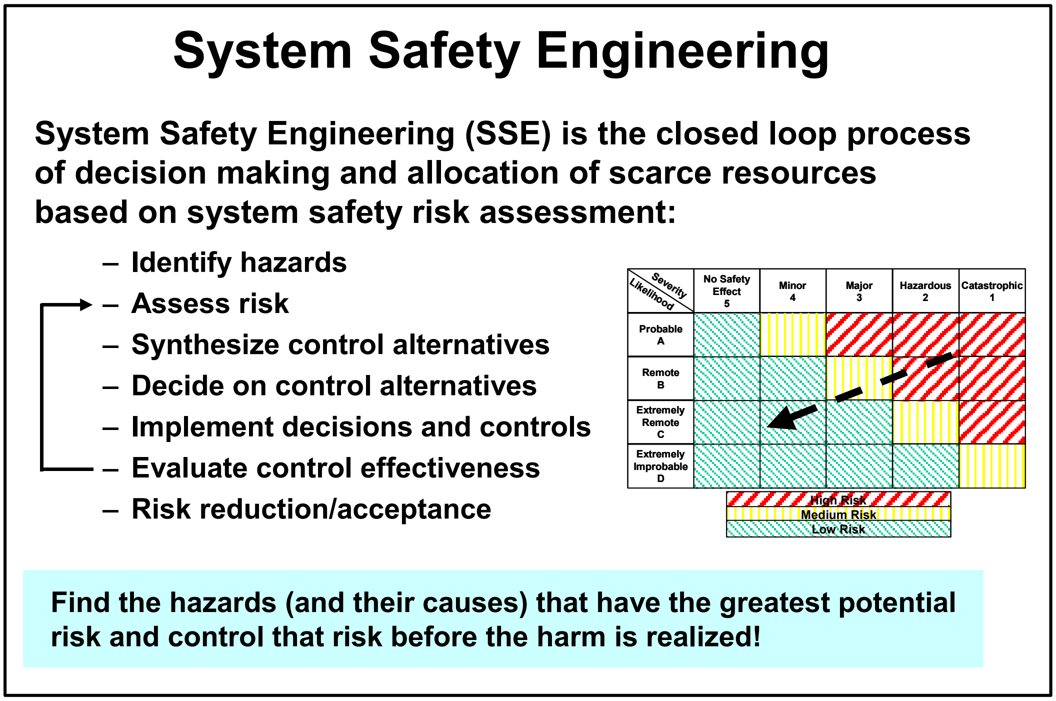

Figure 4.8-4. Closed Loop Nature of System Safety Engineering

To conduct SSE in the AMS, the program performs hazard analyses, as described in the NAS SSMP, Chapters 4 and 5 (http://fast.faa.gov/toolsets/index.htm), and the SSH, Chapter 8 (http://fast.faa.gov/toolsets/index.htm). Figure 4.8-5 shows what safety analyses are performed relative to the phases and decisions of the Integrated Product Development System of the AMS. These safety analyses are timed to best support the phased needs and decisions in the overall AMS process.

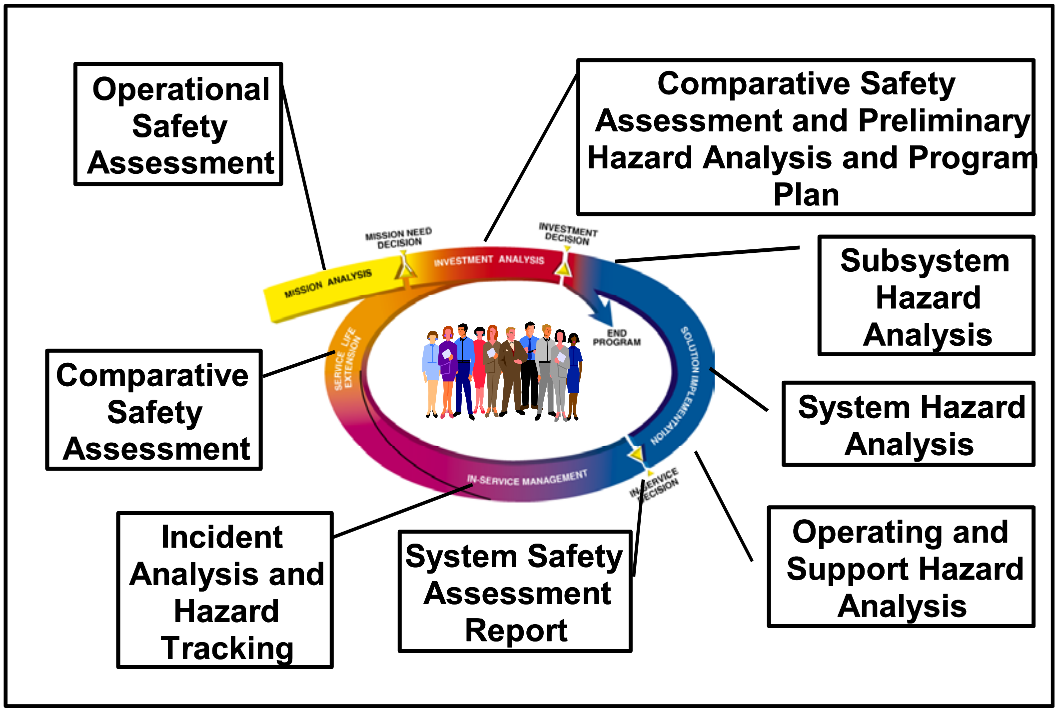

Figure 4.8-5. Types of Safety Hazard Analyses and Their Relative Position in the Acquisition Management System

4.8.1.2 Why Perform System Safety Engineering?

There are two basic reasons for performing SSE on a program:

- To comply with FAA Orders and AMS direction (e.g., FAA Order 8040.4 and AMS, Paragraph 2.9.13)
- To reduce total cost of development and improve program integration

The FAA's primary role is to ensure the safety of the NAS. In performing this role, the FAA has issued FAA Order 8040.4 (http://fast.faa.gov/toolsets/index.htm), which directs all FAA organizations to employ safety risk management in decisionmaking. The AMS was amended to comply with FAA Order 8040.4. The AMS now requires programs to execute system safety and to brief the system safety program status at all Joint Resources Council (JRC) meetings and Acquisition Reviews. The SSH, Chapter 2 (http://fast.faa.gov/toolsets/index.htm), the SSMP, Chapter 6 (http://fast.faa.gov/toolsets/index.htm), and the AMS provide more information on this subject. For example, AMS Paragraph 2.9.13 reads:

> *System Safety Management shall be conducted and documented throughout the acquisition management lifecycle. Critical safety issues identified during mission analysis are recorded in the Mission Need Statement; a system safety assessment of candidate solutions to mission need is reported in the Investment Analysis Report; and Integrated Product Teams provide for program-specific safety risk management planning in the Acquisition Strategy Paper.*

Each line of business involved in acquisition management shall institute a system safety management process that includes, at minimum, the following:

- Hazard identification
- Hazard classification (severity of consequences and likelihood of occurrence)
- Measures to mitigate hazards or reduce risk to an acceptable level
- Verification that mitigation measures are incorporated into product design and implementation
- Assessment of residual risk

Status of system safety shall be presented at all JRCs. The FAST provides detailed guidelines for system safety management (http://fast.faa.gov/toolsets/SafMgmt/IndexStart.htm).

The second reason for conducting safety risk management is that it reduces cost and improves system integration and SE overall.

- System safety looks for programmatic risks that may impact system performance, schedule, and costs.
- System safety finds problems early. As Figure 4.8-6 shows, the earlier in the lifecycle a problem is found and managed, the easier and less expensive it is to correct.

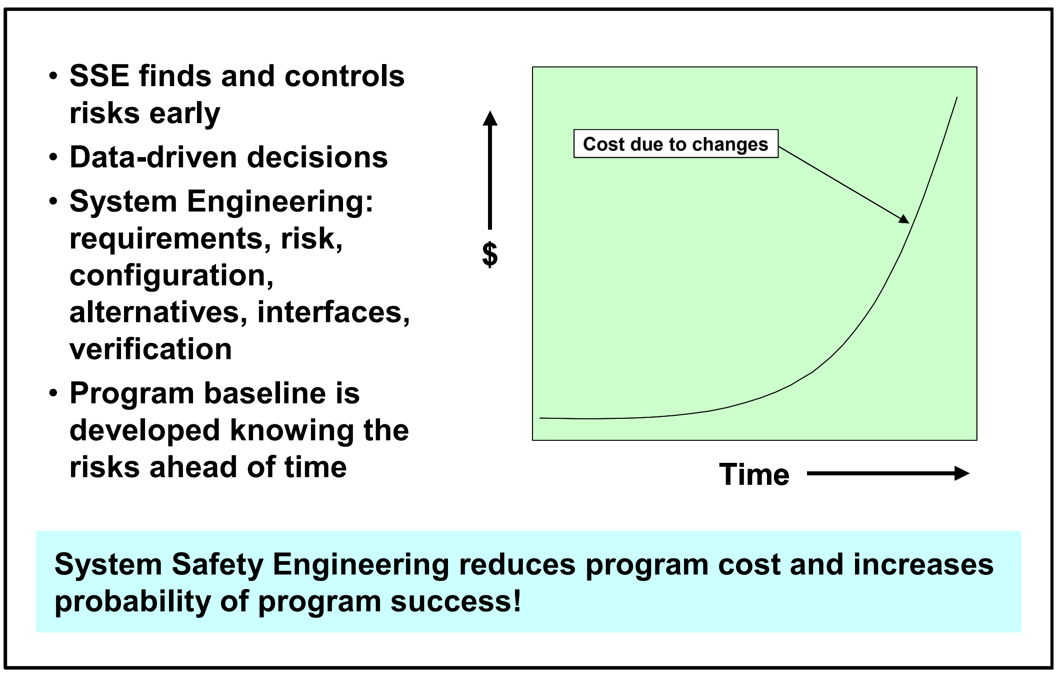

Figure 4.8-6. Benefits of System Safety Engineering

- The outputs of the system safety process feed other SE processes, improving the overall SE of the system (Figure 4.8-7).

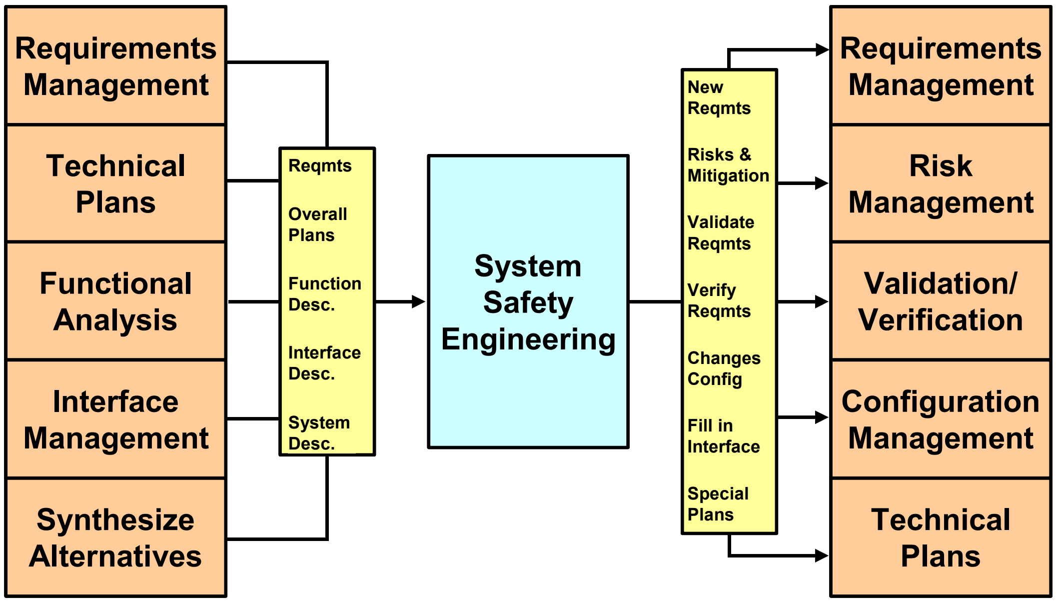

Figure 4.8-7. System Safety Engineering's Relationship to Other System Engineering Processes

4.8.1.3 System Safety Engineering Process Tasks

SSE follows the process tasks outlined in "General Specialty Engineering Process Tasks" (Paragraph 4.8.0.3).

4.8.1.4 System Safety Engineering Outputs/Products

The following products are outputs of SSE.

4.8.1.4.1 Program Planning

Each program is required to have an SSPP. The NAS Modernization SSMP (http://fast.faa.gov/toolsets/index.htm) is the overall plan for conducting safety risk management in the AMS. It is recommended that individual programs consult the SSMP when developing a program-specific SSPP that meets the NAS SSMP requirements. The FAA SSH, Chapter 5 (http://fast.faa.gov/toolsets/index.htm), also provides guidance on this topic.

4.8.1.4.2 Analysis Products

Table 4.8-6 lists the products of SSE. Detailed directions for how to develop these products are referenced in the table.

387 **Table 4.8-6. Products of System Safety Engineering**

System Safety Process Products	How To Reference
Operational Safety Assessment (OSA)	FAA SSH, Chapters 2 and 4 (http://fast.faa.gov/toolsets/index.htm) NAS SSMP, Section 5.2.1 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.1)
Comparative Safety Assessment (CSA)	FAA SSH, Chapters 2 and 4 NAS SSMP, Section 5.2.2 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.2)
Preliminary Hazard Analysis (PHA)	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.3 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.3)
SSPP	FAA SSH, Chapter 5 NAS SSMP, Section 5.2.4 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.4)
SSHA	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.5 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.5)
SHA	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.6 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.6)
O&SHA	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.7 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.7)
Health Hazard Assessment (HHA)	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.8 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.8)
System Safety Assessment Report (SSAR)	NAS SSMP, Section 5.2.9 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.9)
Safety Requirements Verification Table (SRVT)	NAS SSMP, Section 5.2.11 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.11)
Hazard Tracking System	FAA SSH, Section 2.2.3

System Safety Process Products	How To Reference
(HTS)	NAS SSMP, Section 5.2.10 (http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.10)

4.8.2 Reliability, Maintainability, Availability – Reserved

4.8.3 Human Engineering – Reserved

4.8.4 Electromagnetic Environmental Effects – Reserved

4.8.5 Quality Engineering– Reserved

4.8.6 Information Security Engineering – Reserved

4.8.7 Hazardous Materials Management/Environmental Engineering – Reserved